IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE CELLULAR DEVICES ASSIGNED CALL NUMBERS: (617) 828-9060, THAT IS STORED AT PREMISES CONTROLLED BY SPRINT ("TARGET TELEPHONE #11); (617) 230-9781, THAT IS STORED AT PREMISES CONTROLLED BY T-MOBILE ("TARGET TELEPHONE #12");	Case No. 16-mj-6154-MPK, 16-mj-6155-MPK **Filed Under Seal**

SECOND AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, **Shena Latta**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular telephones:

   a. Target Telephone #11 ("TT11") assigned call number (617) 828-9060, that is stored at premises controlled by Sprint Corporation, a wireless telephone service provider headquartered in Overland Park, Kansas that accepts service of process at Sprint Corp., 6480 Sprint Parkway, Overland Park, KS 66251. According to records subpoenaed from Sprint, Target Telephone #11 is currently subscribed by Timothy Torigian, 47 Beethoven Ave, Walpole, Massachusetts 02081.[1] According to records of Sprint, the account has been subscribed since at least from 2012. A preservation request was sent to Sprint Corp. on 02/18/20. The information to be searched is described in the following paragraphs and in Attachment A-11. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require Sprint to disclose to the government copies of the information further described in Section I of Attachment B-11.

[1] That is the address of Lt. Torigian on his 2018 W-2 from BPD.

b. Target Telephone #12 ("TT12") assigned call number (617) 230-9781, that is stored at premises controlled by T-Mobile, a wireless telephone service provider headquartered in Bellevue, Washington that accepts service of process at 4 Sylvan Way, Parsippany, NJ 07054. According to records subpoenaed from T-Mobile, Andre Williams, 25 Teed Road, Holbrook, Massachusetts[2] was the subscriber of Target Telephone #12 from September 2018 through March 2019. A preservation request was sent to T-Mobile on 01/09/20. The information to be searched is described in the following paragraphs and in Attachment A-12. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require T-Mobile to disclose to the government copies of the information further described in Section I of Attachment B-12.

Upon receipt of the information described in Section I of Attachment B11-B12, government-authorized persons will review the information to locate items described in Section II of Attachment B11-12 for each Target Telephone.

2. I am a Special Agent with the Department of Justice, Office of the Inspector General, and have been so employed since September 4, 2018. Prior to this, I served as a Special Agent with the Social Security Administration, Office of the Inspector General for three years and as a Special Agent with the United States Secret Service for over ten years. I am currently assigned to the Boston Area Office and investigate matters related to public corruption as well as those involving fraud, waste and abuse within the Department of Justice. I completed the Federal Law Enforcement Training Center's Criminal Investigator Training Program in Glynco, GA and the United States Secret Service Special Agent Training Academy in Beltsville, MD. I have also received on-the-job training and attended training courses sponsored by multiple federal agencies related to these types of investigations. I have been involved in many complex investigations. I have interviewed defendants, witnesses and victims. I have conducted surveillance, worked with

[2] That is the address of Officer Williams on his 2018 W-2 from BPD.

confidential informants, and participated in investigations using court authorized interception of wire and electronic communications. During my law enforcement career, I have also participated in the preparation and execution of search and arrest warrants. Based upon my training and experience, I am familiar with methods of communication of individuals conducting illegal activity, which include the use of cellular phone communication and records. The facts in this affidavit come from my personal observations, my training and experience, information obtained from subpoenas, public records, other agents, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of: (1) 18 U.S.C. §666, embezzlement from an agency receiving federal funding; (2) 18 U.S.C. §1343, wire fraud; and (3) 18 U.S.C. §371, conspiracy, have been committed by BPD Lt. Timothy Torigian (TT11) and BPD Patrol Officer Andre Williams (TT12), among others.[3] There is also probable cause to search TT11 and TT12 for the information described in Attachment A-11 and A12 for evidence, instrumentalities, contraband, or fruits of these crimes as further described in Attachment B11 and B12.

[3] This Court has previously issued search warrants directing various cell providers to provide location information for cellular phones belonging to Lt. Torigian (that warrant was for a BPD issued phone rather than a personal cellphone), two Sergeants, and seven other officers. *See* Case Nos. 20-mj-2057-MBB to 20-mj-2066-MBB and the First Affidavit of DOJ OIG SA Shena Latta, attached hereto and incorporated in its entirety by reference herein as **Exhibit 1**.

4. The following chart summarizes the allegations of the First Affidavit, **Exhibit 1**, as to each Target Telephone:

Target Telephone (User)	**Specific Examples of False Overtime Claims by the User of the Target Telephone**	**Paragraphs Exhibit 1**	**Total Individual Fraud**
TT11 (Lt. Torigian)	November 23, 2016 January 30, 2017 March 2, 2017 September 7, 2017 October 3, 2017 November 22, 2017 January 11, 2018 February 6, 2018 March 21, 2018 May 29, 2018 June 26, 2018 October 4, 2018 November 15, 2018 December 20, 2018 February 7, 2019	44-47 48-51 52-55 68-71 72-75 76-79 80-83 84-87 88-91 92-95 96-99 104-107 108-111 112-115 116-119	May 2016 to February 2019 – **$43,187 (Ex. 1, ¶138)**
TT12 (PO Williams)	July 27, 2017 October 3, 2017 November 22, 2017 January 11, 2018 February 6, 2018 May 29, 2018 October 4, 2018 December 20, 2018	64-67 72-75 76-79 80-83 84-87 92-95 104-107 112-115	July 2017 to December 2018 – **$11,181 (Ex. 1, ¶165)**

PROBABLE CAUSE

The Boston Police Department Evidence Warehouse

5. As previously detailed in **Exhibit 1**, there is probable cause to believe that members of the Boston Evidence Control Unit have, since at least 2016, conspired to submit, and have submitted, fraudulent overtime slips in order to be paid for hours that they did not work. *See* **Exhibit 1**, ¶¶4-205.

Losses

6. As detailed in **Exhibit 1**, between May of 2016 and February of 2019, members of ECU have been paid over $900,000 for the relevant 4:00 p.m. to 8:00 p.m. overtime shifts.

7. As detailed in **Exhibit 1**, ¶¶133-180, there is probable cause to believe that, cumulatively, between May 2016 and February 2019, the members of the ECU were paid over $250,000 for overtime hours that they fraudulently and falsely claimed to have worked.

8. As detailed in **Exhibit 1**, ¶¶136-138, there is probable cause to believe that Lt. Torigian (user TT11) was paid over $43,187 for overtime hours that he falsely claimed to have worked between May 2016 and February 2019.

9. As detailed in **Exhibit 1**, ¶¶163-165, there is probable cause to believe that Officer Williams (user TT12) was paid over $11,181 for overtime hours that he falsely claimed to have worked between July 2017 and December 2018.

Information Retained by Wireless Providers

10. In my training and experience, providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell

towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.

11. Based on my training and experience, I also know that wireless providers typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

12. Based upon information made available to federal law enforcement by the wireless providers and information maintained by the DOJ for use by law enforcement; (1) T-Mobile routinely maintains up to two years of information relating to the cell towers accessed by a phone; and (2) Sprint routinely maintains up to eighteen months of information relating to the cell towers accessed by a phone.

13. Based on my training and experience, I know that wireless providers typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers typically collect and retain information about their subscribers' use of the wireless service, such as records

about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the user or users of the Target Telephones and may assist in the identification of co-conspirators.

14. In my training and experience, individuals who own and use cellphones keep such cellphones on their persons. Thus, it is reasonable to believe that evidence concerning the location of the cellphone belonging to an individual is relevant to the issue of where the user of that cellphone is located at a given time.

15. Where, as here, there is probable cause to believe that individuals have falsely claimed to have been present at work performing overtime, evidence of the location of the Target Telephones during the period specified in the warrant is likely to be relevant to establishing whether those claims are true (or false).

AUTHORIZATION REQUEST

16. Based on the foregoing, I request that the Court issue the proposed search warrants, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

17. I request that, for TT11 the Court direct Sprint to disclose to the government any information described in Section I of Attachment B-11 that is within its possession, custody, or control. Because the warrant will be served on Sprint, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

18. I further request that, for TT12 the Court direct T-Mobile to disclose to the government any information described in Section I of Attachment B-12 that is within its

possession, custody, or control. Because the warrant will be served on T-Mobile, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

19. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

Respectfully submitted,

SA Shena Latta
Special Agent
Department of Justice,
Office of the Inspector General

Subscribed and sworn to before me on February 20, 2020

M. PAGE KELLEY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-11
Target Telephone #11

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number **(617) 828-9060** ("the Account"), that are stored at premises controlled by Sprint ("the Provider"), headquartered in Overland Park, Kansas that accepts service of process at Sprint Corp., 6480 Sprint Parkway, Overland Park, KS 66251.

ATTACHMENT B-11

Particular Things to be Seized

I. Information to be Disclosed by the Provider

This Order includes all information preserved pursuant to the preservation letter sent to Sprint on 02/18/2020.

To the extent that the information described in Attachment A-11 is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period January 1, 2016 to March 2019:

a. The following information about the customers or subscribers of the Account:

   i. Names (including subscriber names, user names, and screen names);

   ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

   iii. Local and long distance telephone connection records;

   iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

   v. Length of service (including start date) and types of service utilized;

   vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:

i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses);

ii. information regarding the cell tower and antenna face (also known as "sectors") through which the communications were sent and received as well as per-call measurement data (also known as the "real-time tool" or "RTT" data); and

iii. E-911 Phase II data or Global Positioning Device ("GPS") data.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of 18 U.S.C. §371, 18 U.S.C. § 1343; and 18 U.S.C. §666 involving Timothy Torigian, Robert Twitchell, Gerard O'Brien, Darius Agnew, James Carnes, Henry Doherty, Sybil Mason, Kendra Conway, Diana Lopez, Michael Murphy, Ronald Nelson, Andre Williams, Joseph Nee, Thomas Nee, and Kennedy Semedo, during the period **January 1, 2016 through March 2019**. This information includes evidence concerning the location of the

Target Telephone, the location of the user of the Target Telephone, and the identity of the user of the Target Telephone throughout that period.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.

ATTACHMENT A-12
Target Telephone #12

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number **(617) 230-9781**, that are stored at premises controlled by T-Mobile ("the Provider"), headquartered in in Bellevue, Washington that accepts service of process at 4 Sylvan Way, Parsippany, NJ 07054.

ATTACHMENT B-12

Particular Things to be Seized

III. Information to be Disclosed by the Provider

This Order includes all information preserved pursuant to the preservation letter sent to T-Mobile on 01/09/2020.

To the extent that the information described in Attachment A-12 is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period January 1, 2017 to March 2019:

c. The following information about the customers or subscribers of the Account:

   i. Names (including subscriber names, user names, and screen names);

   ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

   iii. Local and long distance telephone connection records;

   iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

   v. Length of service (including start date) and types of service utilized;

   vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

d. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:

i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses);

ii. information regarding the cell tower and antenna face (also known as "sectors") through which the communications were sent and received as well as per-call measurement data (also known as the "real-time tool" or "RTT" data); and

iii. E-911 Phase II data or Global Positioning Device ("GPS") data.

IV. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of 18 U.S.C. §371, 18 U.S.C. § 1343; and 18 U.S.C. §666 involving Timothy Torigian, Robert Twitchell, Gerard O'Brien, Darius Agnew, James Carnes, Henry Doherty, Sybil Mason, Kendra Conway, Diana Lopez, Michael Murphy, Ronald Nelson, Andre Williams, Joseph Nee, Thomas Nee, and Kennedy Semedo, during the period **March 1, 2016 through March 2019**. This information includes evidence concerning the location of the

Target Telephone, the location of the user of the Target Telephone, and the identity of the user of the Target Telephone throughout that period.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.